

In the Claims

1-13. (Cancelled)

14. (Withdrawn) A method comprising:
comparing a user group of a packet with a user group of a destination of said packet.

15. (Withdrawn) The method of claim 14, wherein
said user group of said destination of said packet is identified by a user group identifier,
and
said user group identifier is stored in a role-based access control list entry of an access
control list.

16. (Withdrawn) The method of claim 14, wherein
said user group of said packet is a source user group, and
said user group of said destination of said packet is a destination user group.

17. (Withdrawn) The method of claim 16, wherein
said source user group is assigned to a source of said packet based on a role of said
source, and
said destination user group is assigned to said destination based on a role of said
destination.

18. (Withdrawn) The method of claim 16, further comprising:
retrieving said destination user group from a forwarding information base.

19. (Withdrawn) The method of claim 18, further comprising:
storing said destination user group in an access control list.

20. (Withdrawn) The method of claim 16, wherein
said source user group is indicated by a source user group identifier stored in said packet,
and

said destination user group is indicated by a destination user group stored in a network device receiving said packet.

21. (Withdrawn) The method of claim 16, further comprising:
determining said source user group; and
determining said destination user group by looking up said destination user group in an access control list.

22. (Withdrawn) The method of claim 21, wherein
said destination user group is identified by a destination user group identifier, and
said destination user group identifier is stored in a role-based access control list entry of said access control list.

23. (Withdrawn) The method of claim 21, wherein
said access control list is a role-based access control list.

24. (Withdrawn) The method of claim 21, wherein said determining said source user group comprises:

extracting a source user group identifier from said packet, wherein
said source user group identifier identifies said source user group.

25. (Withdrawn) The method of claim 24, further comprising:
populating said access control list with a destination user group identifier, wherein
said destination user group identifier identifies said destination user group.

26. (Withdrawn) The method of claim 25, wherein
said destination user group is assigned to said destination based on a role of said destination.

27. (Withdrawn) The method of claim 25, wherein
said comparing and said populating are performed by a network device, and
said populating comprises

sending a request to another network device, and
receiving a response from said another network device, wherein
said response includes a destination user group identifier, and
said destination user group identifier identifies said destination user group.

28. (Withdrawn) The method of claim 14, further comprising:
populating a forwarding table with a user group identifier, wherein
said user group identifier identifies said user group of said packet, and
said user group of said packet indicates a user group of a source of said packet.

29. (Withdrawn) The method of claim 28, wherein
said source user group is assigned to said source based on a role of said source.

30. (Withdrawn) The method of claim 28, wherein
said user group is a source user group, and
said user group identifier is a source user group identifier.

31. (Withdrawn) The method of claim 30, wherein
said comparing and said populating are performed by a network device, and
said populating comprises
determining said source user group.

32. (Withdrawn) The method of claim 31, wherein said populating further comprises:
receiving an authentication message from another network device, wherein
said response includes said source user group identifier.

33-54. (Cancelled)

55. (Currently Amended) A method comprising:
populating an access control list with a destination user group identifier, wherein
said destination user group identifier identifies a destination user group of a
destination,

said access control list comprises a source user group field configured to store a source user group identifier and a destination user group field configured to store a destination user group identifier,
said source user group comprises a plurality of source network devices,
said destination user group comprises a plurality of destination network devices, and
said access control list is configured to allow said source user group identifier and said destination user group identifier to be compared.

56. (Original) The method of claim 55, wherein
said destination user group is assigned to said destination based on a role of said destination.

57. (Original) The method of claim 55, wherein
said populating is performed by a network device and comprises
sending a request to another network device, and
receiving a response from said another network device, wherein
said response includes said destination user group identifier, and
said destination user group identifier identifies said destination user group.

58. (Original) The method of claim 55, further comprising:
comparing a user group of a packet with said destination user group.

59. (Original) The method of claim 58, wherein
said user group of said packet is a source user group,
said destination user group is a user group of a destination of said packet, and
said destination is said destination of said packet.

60. (Original) The method of claim 59, wherein
said source user group is assigned to a source of said packet based on a role of said source, and

said destination user group is assigned to said destination based on a role of said destination.

61. (Original) The method of claim 59, wherein
said source user group is indicated by a source user group identifier stored in said packet,
and
said destination user group is indicated by a destination user group stored in a network
device receiving said packet.

62. (Original) The method of claim 59, further comprising:
determining said source user group; and
determining said destination user group by looking up said destination user group in an
access control list.

63. (Original) The method of claim 62, wherein
said access control list is a role-based access control list.

64. (Original) The method of claim 62, wherein said determining said source user
group comprises:
extracting a source user group identifier from said packet, wherein
said source user group identifier identifies said source user group.

65. (Currently Amended) A computer program product comprising:
a first set of instructions, executable on a computer system, configured to populate an
access control list with a destination user group identifier, wherein
said destination user group identifier identifies a destination user group of a
destination,
said access control list comprises a source user group field configured to
store a source user group identifier and a destination user group field
configured to store a destination user group identifier,
said source user group comprises a plurality of source network devices,

said destination user group comprises a plurality of destination network devices, and

said access control list is configured to allow said source user group identifier and said destination user group identifier to be compared; and

computer readable storage media, wherein said computer program product is encoded in said computer readable storage media.

66. (Original) The computer program product of claim 65, further comprising:
a second set of instructions, executable on said computer system, configured to compare
a user group of a packet with said destination user group.

67. (Original) The computer program product of claim 66, wherein
said user group of said packet is a source user group,
said destination user group is a user group of a destination of said packet, and
said destination is said destination of said packet.

68. (Original) The computer program product of claim 67, further comprising:
a third set of instructions, executable on said computer system, configured to determine
said source user group; and
a fourth set of instructions, executable on said computer system, configured to determine
said destination user group by looking up said destination user group in an access
control list.

69. (Original) The computer program product of claim 68, wherein said third set of
instructions comprises:

a first subset of instructions, executable on said computer system, configured to
extracting a source user group identifier from said packet, wherein
said source user group identifier identifies said source user group.

70. (Currently Amended) An apparatus comprising:
means for populating an access control list with a destination user group identifier,
wherein

said destination user group identifier identifies a destination user group of a destination,

said access control list comprises a source user group field configured to store a source user group identifier and a destination user group field configured to store a destination user group identifier,
said source user group comprises a plurality of source network devices,
said destination user group comprises a plurality of destination network devices, and

said access control list is configured to allow said source user group identifier and said destination user group identifier to be compared.

71. (Original) The apparatus of claim 70, further comprising:
means for comparing a user group of a packet with said destination user group.

72. (Original) The apparatus of claim 71, wherein
said user group of said packet is a source user group,
said destination user group is a user group of a destination of said packet, and
said destination is said destination of said packet.

73. (Original) The apparatus of claim 72, further comprising:
means for determining said source user group; and
means for determining said destination user group by looking up said destination user group in an access control list.

74. (Original) The apparatus of claim 73, wherein said means for determining said source user group comprises:

means for extracting a source user group identifier from said packet, wherein
said source user group identifier identifies said source user group.

75. (Withdrawn) A method comprising:
populating a forwarding table with a user group identifier.

76. (Withdrawn) The method of claim 75, wherein said user group identifier is a source user group identifier, and so identifies a source user group.
77. (Withdrawn) The method of claim 76, wherein a source of a packet is in said source user group.
78. (Withdrawn) The method of claim 77, wherein said source user group is assigned to said source based on a role of said source.
79. (Withdrawn) The method of claim 77, wherein said populating comprises determining said source user group.
80. (Withdrawn) The method of claim 79, wherein said populating is performed by a network device and further comprises:
receiving an authentication message from another network device, wherein said response includes said source user group identifier.
81. (Withdrawn) The method of claim 77, wherein a destination of said packet is in a destination user group.
82. (Withdrawn) The method of claim 81, wherein said destination user group is assigned to said destination based on a role of said destination.
83. (Withdrawn) The method of claim 81, further comprising:
comparing a source user group of said packet with said destination user group.
84. (Withdrawn) The method of claim 83, wherein said source user group of said packet is indicated by a source user group identifier stored in said packet, and

said destination user group is indicated by a destination user group stored in a network device performing said comparison.

85. (Withdrawn) The method of claim 81, further comprising:
determining said source user group; and
determining said destination user group by looking up said destination user group in an access control list stored at said network device performing said comparison.

86. (Withdrawn) The method of claim 85, wherein said determining said source user group comprises:
extracting said source user group identifier stored in said packet from said packet,
wherein
said source user group identifier stored in said packet identifies said source user group of said source of said packet.

87-98. (Cancelled)

99. (Withdrawn) A method comprising:
indexing a row of a permissions matrix with a first user group; and
indexing a column of said permissions matrix with a second user group.

100. (Withdrawn) The method of claim 99, wherein
said first user group is a source user group, and
said second user group is a destination user group.

101. (Withdrawn) The method of claim 100, wherein said permissions matrix comprises:
a plurality of permissions matrix entries.

102. (Withdrawn) The method of claim 101, wherein
each of said permissions matrix entries is a pointer to a data structure.

103. (Withdrawn) The method of claim 102, wherein said data structure is a permission list.
104. (Withdrawn) The method of claim 102, wherein said data structure is a permission list entry.
105. (Withdrawn) The method of claim 102, wherein said data structure is a pointer to a permission list.
106. (Withdrawn) The method of claim 105, wherein said data structure further comprises:
another pointer to another permission list.
107. (Withdrawn) The method of claim 102, further comprising:
employing permission list chaining in said data structure.
108. (Withdrawn) The method of claim 102, further comprising:
selecting a selected permissions matrix entry of said permissions matrix entries, wherein
said selecting comprises
identifying a row of said permissions matrix using a source user group identifier,
identifying a column of said permissions matrix using a destination user group
identifier, and
identifying a permissions matrix entry of said permissions matrix entries in said
row and said column as said selected permissions matrix entry.
109. (Withdrawn) The method of claim 108, further comprising:
selecting a permission list from a plurality of permission lists using said selected
permissions matrix entry.
110. (Withdrawn) The method of claim 108, further comprising:
selecting a permission list entry from a permission list using said selected permissions
matrix entry.

111-117. (Cancelled)